AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
HP DESKTOP COMPUTER SERIAL NUMBER 8CG8334JNF CURRENTLY LOCATED AT THE FEDERAL BUREAU OF

Case No. 20-MJ-47-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252	**ACCESS AND ATTEMPT TO ACCESS, WITH INTENT TO VIEW CHILD PORNOGRAPHY**

The application is based on these facts:

See Affidavit of Richard Whisman, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Richard Whisman, SA FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 2-19-20

Judge's signature

City and state: Tulsa, OK

Jodi F. Jayne, U.S. Magistrate
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF: HP DESKTOP COMPUTER SERIAL NUMBER 8CG8334JNF CURRENTLY LOCATED AT THE FEDERAL BUREAU OF INVESTIGATION, TULSA, OKLAHOMA	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Richard Whisman, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, which are electronic devices, currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been for approximately Seventeen years. I am currently assigned to the Tulsa Resident Agency of the Oklahoma City Division. Prior to becoming a Special Agent with the FBI, I was employed for about seven years as a Police Officer with the West Chicago, Illinois Police Department. Since joining the FBI, I have investigated violations of federal law, to include federal violations concerning computer crimes and child exploitation. I have gained experience through training in classes and work related to conducting these types of investigations. Further, as a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

Identification of the Device to be Examined

3. The property item to be searched is a HP desktop computer with serial number 8CG8334JNF. This item is currently in the possession of the Federal Bureau of Investigation in Tulsa, Oklahoma, hereinafter the "Device".

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252 (access, and attempt to access, with intent to view child pornography) are presently located at the subject Device. There is also probable cause to search the Device as described in Attachment A for evidence of these crimes as listed in Attachment B.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

6. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. There were definable costs involved with the production of pornographic images. To distribute these images on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls.

7. The development of computers has changed this; computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

8. Child pornographers can transfer photographs from a camera onto a computer readable format with a device known as a scanner. With the use of digital cameras, the images can be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

9. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The storage capability of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously over the years. These drives can store hundreds of thousands of images at a very high resolution.

10. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

11. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Microsoft, and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e mail services as well as electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

12. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer contains peer to peer software, when the computer was sharing files, and even some of the files which were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

13. A popular tool used by individuals involved in the collection and distribution of child pornography on the Internet, is peer to peer file sharing (hereinafter, "P2P"). P2P file sharing is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. P2P software is readily available for download on the Internet and is often available for free. In general, P2P software allows the user to set-up file(s) on his computer so that the files can be shared with others running compatible P2P software. In essence, a user allows his computer to be searched and accessed by other users of the network. If another user finds a file of interest on his computer, the P2P software allows that other user to download the file from your computer. A user obtains files by opening the P2P software on his computer and typing in a search term or terms. The P2P

software then conducts a search of all computers connected to that network to determine whether any files matching the search term are currently being shared by any other user on that network.

14. P2P file sharing networks, including the eDonkey2000 (hereinafter referred to as "eD2k") network and the Kad network, are frequently used to trade digital files of child pornography. These files include both image and movie files. A commonly used P2P client software program is eMule. eMule is a free software program for the eD2k and Kad file sharing networks.

15. The eD2k file sharing network is composed of clients and servers, the latter commonly referred to as eDonkey or eD2k servers. eMule is a free, publically available open source software program. Typically, when a user launches the eMule software program, the client program will likely connect to an eD2k network server. Once connected to an eD2k server, information about the files the user is sharing is provided to that server. Such information may include the file's eD2k hash value, the file's size, and parsed keyword terms from the file name. The eD2k network uses the MD4 (Message Digest version 4) hash algorithm to uniquely identify files on the network.

16. The eD2k network servers assist the eMule client users in locating files based on the keyword terms searched for by the user. When a user wants to find a file on the eD2k network, the user enters a keyword search into the eMule search screen menu. This initiates a keyword search request to the client's eD2k server, and to other eD2k servers the client is aware of. Each server returns a list of files (not the files themselves) that match the search criteria. This information comes from clients that have recently reported that it had all or part of that file to the eD2k servers. Each file name returned is mapped to an eD2k MD4 hash value, which uniquely identifies the file on the eD2k network. In order for the user to obtain the actual file,

the user must initiate a download process, typically by double clicking on the file name. The user can identify the file(s) they wish download by the file name and/or file type. When the download process of the file actually begins, the download of the file occurs between two or more clients (not the server[s]).

17. Once a user chooses to download a particular file, the eMule client will again query the eD2k servers, though this query is not visible to the user. During this query, the eMule client will essentially ask for the IP addresses of other active clients that either possess this file in whole or in part. The eMule client can then use the Internet Protocol (IP) to directly connect to another client and request the file. Typically, once the eMule client has downloaded part of a file, it may immediately begin sharing the file with other users.

18. In addition to the eD2k network servers, eMule clients can use the Kad network protocols to locate files. Kad differs in that all communication is between clients, rather than relying on servers. In general, the use of a Kad network versus an eD2k network server is transparent to the user. Typically the Kad network and eD2k network operate in parallel to each other and assist with making the P2P file sharing more efficient.

19. The computer running P2P software has an IP address assigned to it while it is connected to the Internet. This address is unique to a particular computer during a specific online session. The IP address provides a unique "location," or address, as to each computer, making it possible for data to be transferred between computers. Investigators are able to see the IP address of any computer system sharing files. Investigators can then search public records that are available on the Internet to determine the specific Internet Service Provider (ISP) who has assigned that IP address to that computer. ISPs maintain logs and records which reflect the specific IP addresses it assigned to specific computers that connect to the Internet through that

ISP at any given moment. Based upon the IP address assigned to the computer sharing files, subscriber information then can be obtained from the ISP which contains identifying information of the individual to whom the account is registered.

20. The computers that are linked together to form the P2P network are located throughout the world; therefore, the P2P network operates in interstate and foreign commerce. A person who includes child pornography files in his/her "shared" folder is hosting child pornography and therefore is promoting, presenting, and potentially distributing child pornography. A person who hosts child pornography is in violation of Title 18, United States Code, Section 2252 in that he/she is promoting and presenting child pornography in interstate and foreign commerce by means of a computer.

Probable Cause

21. On 05/05/2018, I was conducting an on-line Internet investigation to identify those possessing and sharing child pornography using the eDonkey 2000 (eD2k) and Kad networks. I used an eMule Peer to Peer (P2P) file sharing program that limits each download to originate from a single source. An investigation was initiated for a device at IP address 76.254.208.75, because it was associated on the network to one or more files of investigative interest related to child pornography investigations.

22. Through the use of the P2P program I was running, I initiated the download of files from a host computer at IP address 76.254.208.75. I fully downloaded 1 video file and partially downloaded 4 video files from the host computer at IP address 76.254.208.75. The downloads occurred between 05/05/2018 at 3:48 AM and 05 /05/2018 at 4:24 PM. I reviewed the downloaded files and determined that all of the downloaded files appeared to depict child pornography.

23. Below are examples of some of the child pornography files downloaded from IP address 76.254.208.75, listed by filename:

a. **(Kinderkutje) 12Yo Kim Learn 2.avi**: This is a video file that depicts a nude minor girl, possibly around the age of 12. The minor girl is shown touching an adult male's penis and placing the male's penis in her mouth.

b. **Pthc (Kinderkutje) Girl 12Yo pedo ptsc nablot.mpg**: This is a video file that depicts an adult performing oral sex on a minor girl who appears not to have yet reached the age of puberty.

24. An online query of the IP address 76.254.208.75 through the American Registry for Internet Numbers identified the IP address to be registered to AT&T Internet Services. An administrative subpoena was issued to AT&T Internet Services requesting subscriber information for the user of this IP address during the time the files were downloaded on 05/05/2018. The resulting information from AT&T revealed the subscriber was Gregory Kirk, address of 602 North Beaumont Apartment A, Owasso, Oklahoma.

25. On 01/31/2020 myself and Special Agent Rebecca Rogers travelled to 602 North Beaumont Apartment A in Owasso to investigate the above described eMule activity. Agents learned that Kirk no longer lived at the apartment and had moved to another apartment in the same complex, which had the address 603 North Carlsbad Apartment A, Owasso, Oklahoma. Agents knocked on the door of this apartment and it was answered by a male who identified himself as Gregory Kirk. Agents advised Kirk of the nature of their visit and subsequently interviewed Kirk. Through the course of the interview Kirk provided his consent for Agents to search his computer, a HP desktop computer having serial number 8CG8334JNF. A brief search

of the computer revealed about a dozen images of child pornography in the download folder for the eMule program. Kirk denied specifically searching for child pornography and denied knowing the child pornography was saved on his computer. Kirk did admit to inadvertently downloading child pornography, which he claimed to have deleted. Kirk said he uses eMule for adult pornography and for images of clothed minor girls, who Kirk described as models. Kirk's HP desktop computer was taken by Agents and transported to the Tulsa Resident Agency of the FBI, where it has been entered into Evidence.

26. Below is a description of one of the child pornography files located during the search of the HP desktop computer detailed above:

a. Chelda Nackt(10).jpg: This is an image file that depicts a nude minor girl who appeared to have not yet reached the age of puberty. The girl was shown sitting on a pedestal with her legs spread apart, displaying her genitals.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

27. Most individuals who collect child pornography are sexually attracted to children, their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences, including children. Child pornography collectors express their attraction to children through the collection of sexually explicit materials involving children as well as other seemingly innocuous material related to children.

28. These individuals may derive sexual gratification from actual physical contact with children as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for

the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

29. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica" which is defined as any material, relating to children, that serves a sexual purpose for a given individual. It is broader and more encompassing, than child pornography, but at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his intent. It includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

30. Child pornography collectors reinforce their fantasies, often by taking progressive, overt steps aimed at turning the fantasy into reality in some or all of the following ways: collecting and organizing their child-related material; masturbating while viewing the child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need-

driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices, such as a computer and hard drive can store information for long periods of time. Similarly, things that have been viewed via the internet and various software applications are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

33. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited.

34. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

35. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

36. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

37. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

39. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

40. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Richard Whisman
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me on the 19th day of February, 2020

The Honorable Jodi F. Jayne
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property item to be searched is a HP desktop computer serial number 8CG8334JNF, which is currently in the possession of the Federal Bureau of Investigation in Tulsa, Oklahoma.

ATTACHMENT B

Particular Things to be seized

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252, for distributing and accessing, and attempting to access, with intent to view child pornography:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
   a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
   b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
   c. evidence of the lack of such malicious software;
   d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
   e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
   f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
   g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

n. Child pornography and child erotica.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.